JOURNAL OF ALGEBRA 131, 476–482 (1990)

Some Unitary Groups as Galois Groups over $\mathbb{Q}$

GUNTER MALLE*

Mathematisches Institut der Universität Heidelberg, Im Neuenheimer Feld 288, D-6900 Heidelberg, Federal Republic of Germany

Communicated by Leonard Scott

Received April 29, 1989

DEDICATED TO WALTER FEIT ON THE OCCASION OF HIS 60TH BIRTHDAY

In recent years there has been considerable progress in realizing finite groups G as Galois groups over the field of rational numbers $\mathbb{Q}$ or over the maximal abelian extension field $\mathbb{Q}^{ab}$. But the Rationality Criterion [7] used in the proofs has the serious disadvantage that it assumes G to have trivial center. In particular, if G is a nonsplit central extension, even the weaker assumptions for the criteria in [7] do not apply.

A very interesting series of examples of such groups is given by the universal Schur covers $\hat{G}$ of finite simple groups G. Some approaches to realizing these groups $\hat{G}$ as Galois groups are known, though. Serre introduced the method of computing the obstruction to a solution for an embedding problem (i.e., embedding an extension for G into one for $\hat{G}$) via the Hasse–Witt invariant. But this only works for a center of order two and requires the knowledge of a polynomial generating a Galois extension with group G.

Another idea was put forward by Feit [3]. Assume that G has an outer automorphism ρ which can be extended to $\hat{G}$ and then acts nontrivially on $Z(\hat{G})$. If the extended group $\hat{G}: \langle\rho\rangle$ has trivial center, then the usual rationality criteria are applicable, yielding (perhaps) a Galois extension for $\hat{G}: \langle\rho\rangle$. Afterwards an easy descent argument leads to extensions with group $\hat{G}$.

Moreover Feit found conditions for when it suffices to construct a Galois realization for $G: \langle\rho\rangle$ to get one for $\hat{G}: \langle\rho\rangle$, i.e., to solve the embedding problem [3, Lemma 2.7]. He applied this to 3-covers of several sporadic groups and to $2^2 \cdot Sz(8)$. Here we examine the special unitary groups

* The author gratefully acknowledges financial support by the Deutsche Forschungsgemeinschaft.

0021-8693/90 $3.00

$\hat{G} := SU_3(p)$, $2 < p \in \mathbb{P}$, which have a nontrivial center of order three for $p \equiv -1 \pmod 3$. The graph automorphism ρ of order two acts nontrivially on the center of $\hat{G}$. According to the method of Feit, we first study the simple group $G := U_3(p) = \hat{G}/Z(\hat{G})$, extended by the graph automorphism. We find Galois realizations for $U_3(p){:}\,2$ and $U_3(p)$ for $p \equiv -1 \pmod 4$ and $p \equiv 3, 5 \pmod 7$ over $\mathbb{Q}$ (Theorems 1 and 2). Apart from the result of Nauheim [8], who gave realizations for $U_3(p)$ with $p \equiv 7 \pmod{12}$, these groups were not yet known to occur as Galois groups over $\mathbb{Q}$. The criterion of Feit enables us to extend the results to the special unitary groups $SU_3(p)$ (Theorem 3). The verification of the rationality criterion for $U_3(p){:}\,2$ requires the calculation of *normalized structure constants* $n(\mathfrak{C})$ as defined in [7, II, Section 6.1], and hence the determination of some character values of these groups on outer classes. They can not be deduced from the Deligne–Lusztig theory of characters of reductive groups, but have to be computed by using number-theoretic properties of character tables.

1. Some Character Values for $U_3(p){:}\,2$

The group $U_3(2)$ is solvable, and $\mathrm{Aut}(U_3(3)) = G_2(2)$ was already shown to occur as a Galois group over $\mathbb{Q}$ in [6, Theorem 3.4], so we restrict our attention to primes $p > 3$. Then $G = U_3(p)$ is a simple group. It has an outer automorphism ρ of order two, the graph automorphism. We are first interested in the group $H := G{:}\,\langle \rho \rangle$. The application of the Rationality Criterion in [7, II, Section 4.2], necessitates the calculation of a structure constant in H. The character tables of the simple groups $G = U_3(p)$ are known, either from the Deligne–Lusztig theory of characters of groups of Lie type [2], or in this special case also explicitly in [9]. The action of the graph automorphism ρ on the Steinberg generators of G can easily be determined. So the conjugacy classes and characters fixed by ρ are known. Let $\delta = (3, p+1)$ and $\Phi_i = \Phi_i(p)$, the ith cyclotomic polynomial. We will first study a class structure of $G{:}\,2$ which makes use of the special properties of *t.i.*-tori, as demonstrated in [6]. The first class will be the class $2B$ of an outer involution; the second class $4B$ contains elements of order four with centralizer order $|\mathscr{C}_H(4B)| = 2p(p^2-1)$. Finally, let C_T be the class of an element in $H = G{:}\,2$ with order dividing $\Phi_6(p) = p^2 - p + 1$. Then the centralizer of $\sigma \in C_T$ is a cyclic *t.i.*-torus of order $(1/\delta)\,\Phi_6(p)$. Hence the results of [6] apply. In particular, it is easily seen that only the three unipotent characters of G extend to characters of H not vanishing on all three classes of the class structures $\mathfrak{C}_1 = (2B, 4B, C_T)$ and $\mathfrak{C}_2 = (4B, 4B, C_T)$. (For the definition of class structure see [7].) We get Table I.

TABLE I

Some Values of the Unipotent Characters of $U_3(q){:}\,2$

	$1A$	C_T	$2B$	$4B$
$\mathscr{C}$	$\frac{1}{\delta}p^3\Phi_1\Phi_2^2\Phi_6$	$\frac{1}{\delta}\Phi_6$	$p\Phi_1\Phi_2$	$p\Phi_1\Phi_2$
χ_1	1	1	1	1
χ_{cusp}	$p\Phi_1$	-1	·	·
χ_{St}	p^3	-1	p	p

Note. The table gives the centralizer orders in G, not in H (Atlas notation).

PROPOSITION 1. *For the class structures* $\mathfrak{C}_1=(2B, 4B, C_T)$ *and* $\mathfrak{C}_2=(4B, 4B, C_T)$ *of* $H=U_3(q){:}\,2$ *we have* $n(\mathfrak{C}_1)=n(\mathfrak{C}_2)=1$.

Proof. The assertion follows from Table I. The values on the inner classes are taken from [9]. To deduce the values of the extension of the Steinberg character χ_{St}, we mimick Howlett–Lehrer induction. Namely, the trivial character of the normalizer in H of the Borel subgroup of G induced up to H splits into two irreducible components, the trivial character and an extension of the Steinberg character. This yields the values of χ_{St}. Hence only the row for the cuspidal unipotent character χ_{cusp} remains to be computed. For this, let $\chi_{\text{cusp}}(2B)=:a$. Then the structure constant $n(2B, 2B, C_T)=1-a^2/\Phi_1^2$. As the centralizer of the dihedral group generated by a triple from $(2B, 2B, C_T)$ is trivial, the above structure constant has to be a nonnegative integer. Moreover, one easily convinces oneself that the structure constant indeed has to be positive, since the torus T is normalized by the outer automorphism. This proves $a=0$. The same calculation for $b:=\chi_{\text{cusp}}(4B)$ shows $b\in\{0, \pm\Phi_1\}$. We will determine the correct value for b in the proof of Proposition 2. Assuming $b=0$, the table and the proposition are proved. ∎

We will now study another class structure of H, which does not contain elements of a *t.i.*-torus. We need the two classes pA and pB of p-elements of G fixed by the outer automorphism; the values of the characters on these classes can be taken from [9]. The outer class $4B$ was already introduced before. Elements in $2pB$ have order $2p$ and generate a selfcentralizing cyclic subgroup. Finally, $4pB$ and $4pC$ are the two classes of outer elements of order $4p$. We list all the irreducible characters of G extending to H in Table II, together with their values on some classes of H. There are the unipotent characters χ_1, χ_{cusp}, and χ_{St}, two characters belonging to the semisimple class of involutions, one character from an element of order three, and two families of Deligne–Lusztig characters $R_{|T|}$ belonging to a maximal torus T.

The class structure is chosen to be $\mathfrak{C}_3=(4B, 2pB, pA)$.

TABLE II

Some Values of the Extending Characters in $U_3(p)$: 2, $p \equiv -1 \pmod 4$

Number of characters	$\mathscr{C}$	$1A$ $\lvert G\rvert$	pA $\frac{1}{\delta}p^3\Phi_2$	pB p^2	$4B$ $p\Phi_1\Phi_2$	$2pB$ p	$4pBC$ $2p$
1	χ_1	1	1	1	1	1	1
1	χ_{cusp}	$p\Phi_1$	$-p$	·	·	·	$\sqrt{-p}$
1	χ_{St}	p^3	·	·	p	·	·
1	$\chi_{2,1}$	Φ_6	$-\Phi_1$	1	$-p$	1	·
1	$\chi_{2,\text{St}}$	$p\Phi_6$	p	·	-1	·	-1
1	$\chi_{3,1}$	$\frac{1}{\delta}\Phi_1\Phi_6$	$\frac{1}{\delta}(2p-1)$	$\frac{\delta-1}{3}\Phi_2-1$	$-\Phi_1$	1	1
$\frac{p-3}{2}$	$R_{\Phi_2^2}$	$\Phi_1\Phi_6$	$2p-1$	-1	$\pm\Phi_1$	1	∓ 1
$\frac{p-3}{2}$	$R_{\Phi_1\Phi_2}$	$\Phi_2\Phi_6$	1	1	$\pm\Phi_2$	1	± 1

PROPOSITION 2. *For the class structure* $\mathfrak{C}_3 = (4B, 2pB, pA)$ *of* $H = U_3(p)$: 2 *with* $p \equiv -1 \pmod 4$, *we have* $n(\mathfrak{C}_3) = 1$.

Proof. The value of $n(\mathfrak{C}_3)$ follows immediately from Table II. So we only have to compute the values of the characters in the table on the outer classes. Although the classes $4pB$ and $4pC$ do not occur in the class structure, their character values are needed to determine those on the class $4B$. First we study the values on $2pB$. The squares of elements from $2pB$ lie in pB, hence by known congruences for character values we have $\chi(2pB) \equiv \chi(pB) \pmod 2$ for every irreducible character χ of H. By inspection, $\chi(pB) \equiv 1 \pmod 2$ and hence $\chi(2pB)^2 \geqslant 1$ for at least p different characters of G. But $\sum |\chi(2pB)|^2 = |\mathscr{C}_H(2pB)| = 2p$, and hence these are the only characters not vanishing on $2pB$, and all take value 1 or -1. As we list only one character of each pair of extensions from G (Atlas notation), the column for $2pB$ in Table II follows.

Next we induce up characters from the normalizer in H of the Borel subgroup of G. It has the structure $N := [p_3]\colon (p^2-1)/\delta\colon 2$. The linear characters of N (i.e., the characters of the cyclic commutator factor group of order $2(p-1)$ induced up to H stay irreducible, apart from the trivial character and a character belonging to an element of order two. The latter decompose into $\chi_1 + \chi_{\text{St}}$, $\chi_{2,1} + \chi_{2,\text{St}}$ respectively, as can be seen from the decomposition of characters induced from the Borel subgroup to G [2]. This yields the values for $R_{\Phi_1\Phi_2}$ (the characters remaining irreducible) and χ_{St}.

The classes $4pB$ and $4pC$ are algebraically conjugate over the field $\mathbb{Q}(\sqrt{-p})$. This irrationality is independent of those occuring in the character table of G. Hence any character χ of H taking nonrational values on $4pBC$ is algebraically conjugate to $\chi \cdot \chi_{\text{sign}}$, with χ_{sign} the sign character of H. In particular any such character vanishes on rational outer classes. By our knowledge of the column for $2pB$ and the values of χ_{St}, only χ_{cusp} or $\chi_{2,\text{St}}$ satisfy this condition. But the sum of $\chi_{2,1}$ and $\chi_{2,\text{St}}$ is rational (see above), hence $\chi_{2,\text{St}}$ is as well. So χ_{cusp} is the irreducible character taking nonrational values on $4pBC$, and hence vanishes on the rational class $4B$. Note that up to now we did not need $p \equiv -1 \pmod 4$, so this closes the gap in the proof of Proposition 1.

As $(4pB)^p = 4B$, we must have $\chi_{\text{cusp}}(4pB) \equiv 0 \pmod{\wp}$, with $\wp \mid p$ in $\mathbb{Q}(\sqrt{-p})$. Moreover $\chi_{\text{cusp}}(4pB) \equiv 1 \pmod 2$ due to $(4pB)^4 = pA$, and a short calculation yields the value given in the table. Now we can deduce the other values on $4pB$ as in the case of $2pB$. Namely, congruences to the values on pA and the condition on the sum of the squares force the rest of the row for $4pB$.

Finally, we have enough data to compute the values on the class $4B$. Using $(4pB)^p = 4B$ we get $\chi(4B) \equiv \pm 1 \pmod p$ and from $(4B)^4 = 1A$, also $\chi(4B) \equiv 0 \pmod 2$ for $\chi \in \{\chi_{3,1}, R_{\Phi_2^2}\}$. This forces $\chi(4B)^2 \geqslant \Phi_1^2$ on all those characters. Calculating the sum of the squares of the character values and remembering $\chi_{2,1}(4B) + \chi_{2,\text{St}}(4B) = -\Phi_2$, $\chi_{2,1}(4B) \equiv 0 \pmod p$, only the values in the table satisfy all requirements. The signs are determined from the orthogonality to the column for $2pB$. In particular, if $p \equiv -1 \pmod 4$, the value of $\chi_{2,1}$ is $-p$, and there are as many negative signs as positive ones hidden by the $\pm$ in the table. (If $p \equiv 1 \pmod 4$, we would get $\chi_{2,1}(4B) = p$, and the structure constant is equal to zero.) The formula for the normalized structure constant now gives $n(\mathfrak{C}_3) = 1$. ∎

2. The Galois Realizations

To obtain Galois realizations over $\mathbb{Q}$, the class structures $\mathfrak{C}$ have to be rational. The classes pA, $2B$, $4B$, $2pB$ are rational for all primes $p > 3$. But elements in C_T are conjugate to only six of their primitive powers, hence C_T is rational iff it contains elements of order seven. This can only happen if $7 \mid \Phi_6(p)$, i.e., if $p \equiv 3, 5 \pmod 7$. Writing $7A := C_T$ in this case we arrive at

THEOREM 1. (a) *The groups $U_3(p){:}2$, $p \equiv 3, 5 \pmod 7$, $p > 5$, occur as Galois groups over $\mathbb{Q}(t)$ and over $\mathbb{Q}$ for the ramification structures $\mathfrak{C}_1^* = (2B, 4B, 7A)^*$ and $\mathfrak{C}_2^* = (4B, 4B, 7A)^*$.*

(b) *The groups $U_3(p){:}2$, $p \equiv -1 \pmod 4$, $p > 3$, occur as Galois groups over $\mathbb{Q}(t)$ and over $\mathbb{Q}$ for the ramification structure $\mathfrak{C}_3^* = (4B, 2pB, pA)^*$.*

Proof. In both cases we already know $n(\mathfrak{C}) = 1$ by Propositions 1 and 2. It therefore remains to prove that a triple from any class structure generates H. Let first $K = \langle \sigma_1, \sigma_2, \sigma_3 \rangle$ with $(\sigma_1, \sigma_2, \sigma_3) \in \bar{\Sigma}(\mathfrak{C}_1)$. Then by the list [4] of maximal subgroups of G, elements σ_3 from the *t.i.*-torus T of order $\Phi_6(p)$ are contained either in $\mathcal{N}_G(T) = T{:}\,3$, in an $L_2(7)$, or for $p=5$ in an A_7. But $\mathcal{N}_H(T) \cong T{:}\,6$ has no $(2, 4, 7)$-system, excluding this case. Now assume $K \leqslant PGL_2(7) = \mathcal{N}_H(L_2(7))$. Then in $PGL_2(7)$ there would exist a $(2, 4, 7)$-system of elements, with the first two lying in $PGL_2(7) \backslash L_2(7)$. But there are no outer elements of order four in $PGL_2(7)$. Finally, the case $p=5$ (and hence the possibility $K \leqslant S_7 = \mathcal{N}_H(A_7)$) is excluded in the theorem. The same arguments apply for a triple from the second class structure $\mathfrak{C}_2$. The first part of the theorem then follows from [7, II, Section 4.2, Folgerung 3], and from using the Hilbert irreducibility theorem to descend to $\mathbb{Q}$.

In the second case, let again $K = \langle \sigma_1, \sigma_2, \sigma_3 \rangle$ for $(\sigma_1, \sigma_2, \sigma_3) \in \bar{\Sigma}(\mathfrak{C}_3)$. As σ_2^2 lies in another p-class than σ_3, the Sylow p-subgroup of K has order at least p^2. It cannot be normal in K, for otherwise the factor group $\bar{K}$ would have a $(4, 2)$ generating system, which is impossible. We now consult the list of Kleidman [4] of maximal subgroups of the three dimensional unitary groups. Obviously, no candidate but $H = K$ remains for the group generated by the triple of elements. So the second part also follows with [7]. ▮

From this theorem, Galois realizations of some related groups can be derived. First we descend to the normal subgroup G of index 2.

THEOREM 2. *The simple groups $U_3(p)$ with $p \equiv 3, 5 \pmod 7$, $p > 5$, (resp. $p \equiv -1 \pmod 4$, $p > 3$) occur as Galois groups over $\mathbb{Q}(t)$ and over $\mathbb{Q}$ for the ramification structures $\mathfrak{C}_4^* = (2A, 7A, 7B)^*$ and $\mathfrak{C}_5^* = (2A, 2A, 7A, 7B)^*$ (resp. $\mathfrak{C}_6^* = (2A, pB, pA, pA)^*$).*

Proof. This follows by an easy argument as for example in [7, II, Section 3.2], by proving the rationality of the fixed field of $U_3(p)$ in the $\mathbb{Q}(t)$-extension for $U_3(p){:}\,2$. ▮

For congruences $p \equiv 1 \pmod 3$, $U_3(p)$ has no outer automorphisms apart from the graph automorphism. Hence the Galois extensions in Theorem 1 are GAR realizations in the sense of [7, IV, Section 4]. In the other cases there exist further outer automorphisms, but we can then apply the criterion of Feit [3] to get the universal Schur covers as Galois groups over $\mathbb{Q}$.

THEOREM 3. *For primes $p > 5$ with $p \equiv 3, 5 \pmod 7$ or $p \equiv -1 \pmod 4$, the universal Schur covers $SU_3(p)$ of the projective unitary groups $U_3(p)$*

occur as Galois groups over $\mathbb{Q}(t)$ and over $\mathbb{Q}$. The corresponding class structures are inverse images of the class structures for $U_3(p)$ in Theorem 2 *under the canonical homomorphism.*

Proof. If $p \equiv 1 \pmod 3$, the universal cover is equal to the simple group, and nothing is left to prove. So assume $p \equiv -1 \pmod 3$. Then an application of Lemma 2.7 of Feit [3] to the Galois realizations for $U_3(p){:}\,2$ first gives Galois realizations with groups $3 \cdot U_3(p){:}\,2$; then the descent argument is used to arrive at $SU_3(p) = 3 \cdot U_3(p)$. ∎

It should be noted that the class structures naturally correspond to the ones considered by Thompson [10] and some of those in [5] for the projective special linear groups $L_3(p)$ (i.e., they can be obtained by formally "replacing p by $-p$" where relevant).

References

1. M. Aschbacher, D. Gorenstein, R. Lyons, M. O'Nan, L. Sims, and W. Feit (Eds.), "Proceedings of the Rutgers group theory year, 1983–1984," Cambridge Univ. Press, London, 1984.
2. R. W. Carter, "Finite Groups of Lie Type: Conjugacy Classes and Complex Characters," Wiley, Chichester, 1985.
3. W. Feit, Some finite groups with centers which are Galois groups, *in* "Group Theory, Proceedings of the 1987 Singapore Conference," de Gruyter, Berlin/New York, 1989.
4. P. Kleidman, The low-dimensional classical groups and their subgroups, to appear in *Longman Res. Notes*, in press.
5. G. Malle, "Realisierung von Gruppen $PSL_2(\mathbb{F}_p)$ und $PSL_3(\mathbb{F}_p)$ als Galoisgruppen über $\mathbb{Q}$," Diplomarbeit, Math. Fak. Univ. Karlsruhe (TH), 1985.
6. G. Malle, Exceptional groups of Lie type as Galois groups, *J. Reine Angew. Math.* **392** (1988), 70–109.
7. B. H. Matzat, "Konstruktive Galoistheorie," Lecture Notes in Mathematics, Vol. 1284, Springer-Verlag, Berlin/New York, 1987.
8. R. Nauheim, "Realisierung unitärer Gruppen als Galoisgruppen über $\mathbb{Q}$, Diplomarbeit, Math. Fak. Univ. Karlsruhe (TH), 1988.
9. W. Simpson and J. Frame, The character tables for $SL_3(q)$, $SU_3(q)$, $PSL_3(q)$, $U_3(q)$, *Canad. J. Math.* **25** (1973), 486–494.
10. J. G. Thompson, PSL_3 and Galois groups over $\mathbb{Q}$, in [1].